UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

STONES GROUP INC. and STONEX FINANCIAL INC.,

Plaintiffs,

-against-

HOWARD SHIPMAN,

Defendant.

Case No. _ _ _ _ _ _ _

DECLARATION OF R. CUYLER ROBINSON

1. I, R. Cuyler Robinson, declare under penalty of perjury that the following is true, based upon my personal knowledge. I personally performed, supervised, or reviewed the forensic examinations by Charles River Associates ("CRA") described in this declaration. If called to do so, I can and will testify as follows:

Qualifications

2. I am a Vice President in the Forensic Services practice at CRA. CRA is a global consulting firm with over 850 professionals specializing in providing economic, accounting, financial, and management consulting services. CRA offers economic, financial and business management expertise to major law firms, businesses, accounting firms and governments.

3. I have over twenty years of professional experience in the field of information technology and information security including over fifteen years of professional experience in incident response and digital forensics. A copy of my curriculum vitae is attached as Exhibit A.

4. I possess certifications that relate to information security, data privacy, computer forensics, and incident response. The certifications required formal training and earning a passing score on a formal exam. Each certification also requires that I receive relevant

continuing professional education annually.

5. I have investigated hundreds of matters involving data security incidents and matters where confidential, trade secret information was misappropriated or alleged to have been misappropriated. My work on these matters over the past seventeen years have given me valuable insight into the risk of trade secret misappropriation, the methods by which trade secrets are misappropriated, and internal company procedures that reduce this risk. I have served as an independent forensic neutral expert in multiple matters where either the Court and/or the parties agreed that I would be designated to provide various evidence preservation and forensic analysis services.

Background

6. Upon information and belief, on December 9, 2022 at approximately 3:30 pm CT, I understand that StoneX Group, Inc. ("StoneX") notified Howard Shipman ("Shipman") that his employment with StoneX would be terminated, effective immediately.

7. Upon information and belief, on December 9, 2022 at 3:09 pm CT, StoneX disabled Shipman's Microsoft Windows user account due to Shipman's termination.

8. CRA was retained on December 27, 2022 by Proskauer Rose LLP on behalf of StoneX to forensically investigate StoneX computers used or accessed by Shipman.

9. In this declaration, I will describe how Shipman destroyed StoneX data from StoneX computers after he learned that his employment would be terminated. Furthermore, I will describe other storage locations where Shipman copied StoneX data that StoneX is unable to access. These locations include two personal USB storage drives and a cloud storage computer operated by Linode, LLC.

Evidence and Analysis

10. CRA collected forensic evidence from StoneX computers and systems. This

included the following evidence.

11. On January 2, 2023, CRA collected from StoneX other computer system logs and records associated with Shipman that are more specifically described below.

12. On January 3, 2023, CRA received a laptop that was shipped to CRA via FedEx. RA was informed by Proskauer that the laptop was owned by StoneX, assigned to Shipman, and was shipped to CRA by counsel representing Shipman. The laptop was a Dell Precision 7540 with serial number FCL0833 ("Shipman's Laptop").

13. On January 4, 2023, CRA received a copy of a StoneX virtual computer. The virtual computer was hosted within a Microsoft Azure cloud environment operated by StoneX. The virtual computer was named "CORVO-004" and was used by Shipman for StoneX work purposes ("Corvo-004 Server").

14. CRA used forensic software to examine the collected forensic evidence. Forensic software is used to search for and recover files and folders, identify and interpret artifacts that show computer and user activity, and perform other computer investigative tasks.

Chronology of Events after Shipman's Termination

15. CRA determined the following events occurred after Shipman was notified that his employment was terminated at 3:30 pm CT.

16. I determined that despite disabling Shipman's Microsoft Windows user account, Shipman was still able to access StoneX computers within StoneX's Microsoft Azure development environment. The StoneX computers within this environment were accessible through network connections and other local accounts that were under Shipman's control. Furthermore, I determined that disabling Shipman's Microsoft Windows user account did not prevent Shipman from accessing Shipman's Laptop. Shipman's Microsoft Windows user account disablement was not synchronized to Shipman's Laptop.

17. On December 9, 2022 at 4:05 pm CT, a Microsoft Azure Defender security alert reported that the "bash_history" for the "pianoman" account on the Corvo-004 Server was deleted. I understand from StoneX that pianoman was the user account that Shipman created and used to access StoneX computers in the Microsoft Azure environment. Bash_history stores a record of commands that have recently been issued to by a user.

18. On December 9, 2022 at 4:13 pm CT, a second Microsoft Azure Defender security alert reported that the bash_history for the "root" account on the Corvo-004 Server was deleted. The root account is the default and primary administrator account on Linux computers.

19. Other artifacts recovered from Corvo-004 confirmed that the bash_history for the pianoman and root accounts were cleared using the "VIM" text editor program. Additionally, based on a VIM text editor program log file, user folders under the pianoman account, including Desktop, Downloads, and Documents, were deleted on December 9, 2022 around 4:14 pm CT.

20. Clearing the bash_history and deleting the Desktop, Downloads, Documents and other folders destroyed data on the Corvo-004 Server. More specifically, clearing bash_history obfuscated any commands Shipman may have issued on Corvo-004 using the pianoman or root accounts. If Shipman issued commands to access other cloud computers or StoneX source code, these commands were destroyed.

21. On December 10, 2022 at 10:55:15 am CT, a SanDisk drive was connected to Shipman's Laptop. Shipman's Laptop assigned the SanDisk drive a device name of "SanDisk Cruzer Glide USB Device" and an internal serial number of "20042605701683737105". The storage volume on the SanDisk drive was named "UBUNTU-SERV".

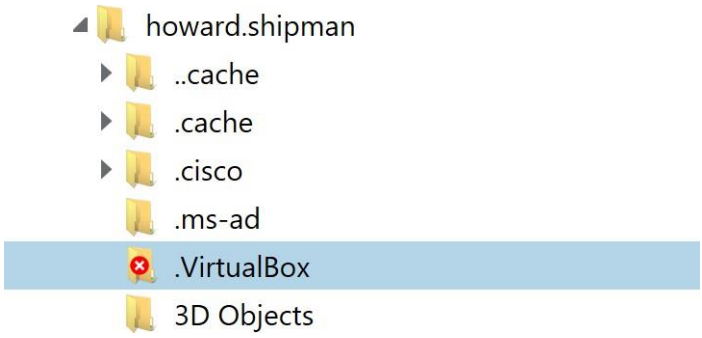
22. On December 13, 2022 at 11:47:47 pm CT, the SanDisk drive was connected to Shipman's Laptop. At 11:49:54 pm CT, a "D:\StoneX Docs" folder was created on the SanDisk drive. From 11:50:34 pm between 11:51:31 pm CT, the following folders were created on the

SanDisk drive within the StoneX Docs folder:

Timestamp CT	Event	Path
12/13/22 11:50:34 PM	Created	D:\StoneX Docs\SIP
12/13/22 11:50:35 PM	Created	D:\StoneX Docs\Travel
12/13/22 11:50:35 PM	Created	D:\StoneX Docs\Texas
12/13/22 11:50:45 PM	Created	D:\StoneX Docs\Baml
12/13/22 11:50:46 PM	Created	D:\StoneX Docs\Budget
12/13/22 11:50:47 PM	Created	D:\StoneX Docs\Darwin
12/13/22 11:50:47 PM	Created	D:\StoneX Docs\Custom Office Templates
12/13/22 11:50:47 PM	Created	D:\StoneX Docs\Candidates
12/13/22 11:51:01 PM	Created	D:\StoneX Docs\HPC
12/13/22 11:51:01 PM	Created	D:\StoneX Docs\Data
12/13/22 11:51:02 PM	Created	D:\StoneX Docs\OnixS
12/13/22 11:51:02 PM	Created	D:\StoneX Docs\OneNote Notebooks
12/13/22 11:51:30 PM	Created	D:\StoneX Docs\Research
12/13/22 11:51:30 PM	Created	D:\StoneX Docs\Personal
12/13/22 11:51:30 PM	Created	D:\StoneX Docs\Outlook Files
12/13/22 11:51:31 PM	Created	D:\StoneX Docs\Security Standards

23. The folders were created on the SanDisk drive in succession and within seconds of each other. I searched Shipman's Laptop for these folders but was unable to locate or forensically recover these folders or data they may have contained. Based on my experience, this activity is consistent with copying folders (and their contents) to the SanDisk drive using Shipman's Laptop.

24. On December 14, 2022 at 12:00:35 am CT, a "C:\Users\howard.shipman\.VirtualBox" folder and any files it contained was deleted from Shipman's Laptop.



25. VirtualBox is a software program that creates and runs virtual versions of computers. Based on my experience, any virtual computers and information about those virtual computers are typically stored within the VirtualBox folder that was deleted.

26. On December 14, 2022 at 12:01:48 am CT, the SanDisk drive was disconnected from Shipman's Laptop. The SanDisk drive was connected at the time that the VirtualBox folder was deleted and then disconnected one minute and thirteen seconds later.

27. On December 14, 2022 at 9:08:27 pm CT, the SanDisk drive was again connected to Shipman's Laptop. It was disconnected about 5 seconds after it was connected.

28. On December 23, 2022 at 2:39 pm CT, all Google Chrome web history was cleared from Shipman's Laptop. Clearing the web history removes the history of web sites that were visited, saved passwords, and other web browser data and settings. CRA was unable to recover any Google Chrome external web browsing history data from Shipman's Laptop because it was cleared.

29. On December 26, 2022 at 3:45:53 pm CT, a Sony drive was connected to Shipman's Laptop. The Sony drive had previously been connected to Shipman's Laptop on December 5, 2022 at 1:26:24 pm CT. Shipman's Laptop assigned the Sony drive a device name of "Sony Storage Media USB Device" and an internal serial number of "7&388e6bd2."

30. Sixty-three seconds after the Sony drive was connected to Shipman's Laptop, two files were accessed. The files "C:\Users\howard.shipman\Documents\Darwin\QuantStrat Plan 2023.docx" and "C:\Users\howard.shipman\Documents\mm_shares.xlsx" were accessed at exactly the same time on December 26, 2022 at 3:46:56 pm CT. No other files were accessed during this timeframe. Based on my experience, these artifacts are consistent with the two files

being copied to the Sony drive. The Sony drive was then removed from Shipman's Laptop on December 26, 2022 at 4:06:15 pm CT.

Linode Computer

31. I determined that the StoneX Corvo-004 Server had been connected to a Linode cloud computer.

32. Linode is a cloud computer company that provides Linux virtual machines to its customers. A customer can sign up for a Linode account at Linode.com and then create and configure computers that will be hosted by Linode.

33. Between August 16, 2022 and December 9, 2022, over two-hundred secure shell protocol ("SSH") connections were made to the Corvo-004 Server with the username pianoman from IP address [redacted][1] According to its American Registry for Internet Numbers (ARIN) record, the computer with the [redacted] IP address was registered to Akamai Technologies, Inc. and is associated with Linode (the "Linode Cloud Computer").[2]

34. I reviewed multiple Linux artifacts and log files from the Corvo-004 Server that collectively indicate StoneX data existed on the Linode Cloud Computer.[3] Specifically, from my analysis, I determined that Corvo-004 Server and the Linode Cloud Computer were connected through SSH and a data volume on the Linode Cloud Computer was mounted to the Corvo-004 Server. Other artifacts showed that within this mounted data volume were multiple files and

[1] SSH is a protocol used to connect computers over a network.
[2] In March 2022, Akamai acquired Linode. See https://www.akamai.com/newsroom/press-release/akamai-completes-acquisition-of-linode, Last Visited: January 12, 2023.
[3] The Linux artifacts I reviewed include a viminfo configuration file, an xsession error log, the file system table, authentication logs, and the system log.

based on file name these files appear to be StoneX source code files. A list of the specific files I identified that likely existed on the Linode Cloud Computer can be seen in the figure below.

.viminfo Files
/mnt/data1/projects/test/share/research/darwin/src/fitzroy/loaders/FitzRoyLoader.hpp
/mnt/data1/projects/test/share/research/darwin/makefile
/mnt/data1/projects/test/share/research/darwin/src/makefile
/mnt/data1/projects/test/share/research/darwin/src/forge/ForgeMode.cpp
/mnt/data1/projects/darwin/bin/RunSim.sh
/mnt/data1/projects/darwin/etc/syms.256.list
/mnt/data1/projects/darwin/bin/RunTest.sh
/mnt/data1/projects/darwin/bin/RunFit.sh
/mnt/data1/projects/darwin/bin/RunSample.sh
/mnt/data1/projects/darwin/DelMe.cpp
/mnt/data1/projects/durango/scripts/install_node/InstallNodePackages.sh
/mnt/data1/projects/darwin/etc/samples.list

Limitations of Evidence

35. The forensic artifacts I reviewed allowed me to identify certain files and folders that existed on or were likely copied to the SanDisk drive, Sony drive, or the Linode Cloud Computer. The forensic artifacts I reviewed are limited in that they did not identify all files and folders that existed on the SanDisk drive, Sony drive, or the Linode Cloud Computer. To determine if other StoneX data was copied to the SanDisk drive, Sony drive, Linode Cloud Computer, or any other computer, device, or account in Shipman's possession or control, I would need direct access to forensically examine those computers, devices, or accounts.

VERIFICATION

Pursuant to 28 U.S.C. § 1746, I verify under penalty of perjury that the foregoing is true and correct.

EXECUTED on this 13th day of January 2023

R. Cuyler Robinson